State of Arizona

	Department of Economic Security Information Technology Standards	Title: 1-38-0019 DES Virus Protection Standard	
Subject: This standard identifies software to be used to protect against viruses and other malicious code that may infect information, data, and programs on information technology systems within DES.		***Effective Date:***	***Revision:***
		07/28/2000	1.4

1. **Summary of Standard Changes**
   1.1. 11/02/01 – Results of an annual review. No substantive changes were implemented.
   1.2. 03/22/02 – Change to Network Associates/McAfee only.
   1.3. 04/03/03 – Changes resulting from the DES Remote Access and Telecommuting Study.
   1.4. 05/11/04 – Text added about patching software products.

2. **Purpose**
   This standard identifies specific software products and procedures intended to aid DES in eliminating viruses and other malicious code that may infect information, data, and programs on information technology systems within DES.

3. **Scope**
   3.1. This standard applies to all DES administrative entities, councils, divisions, administrations, and programs.
   3.2. This standard applies to telecommuters, vendors, service providers, and all governmental and non-governmental entities that are granted access to DES computing environments and/or data, whether connected locally or remotely.

4. **Responsibilities**
   4.1. The DES Director, Deputy Directors, Associate Directors, and Assistant Directors are responsible for enforcing this standard.
   4.2. The DES CIO is responsible for implementing agency policy and standards regarding virus and malicious code prevention, detection, recovery and the reporting of such results to agency management.
   4.3. The DES Division of Technology Services is responsible for implementing this standard and monitoring DES compliance.
   4.4. GITA is responsible for tracking and monitoring virus and malicious code programs and assisting State agencies, when requested, to prevent virus attacks on information technology systems.

5. **Definitions and Abbreviations**
   5.1. **Definitions**
      5.1.1. **Anti-Virus programs** are programs that prevent the infection and replication process from happening on computers, networks, operating, and communications systems.
      5.1.2. **Information Technology Systems** - Equipment used to create, store and transmit digital data and any related software owned (or otherwise controlled) and used by the DES and its divisions and programs to fulfill its service and obligations to the citizens of Arizona.

Definitions (continued)

5.1.3. **Program Code** - A set of instructions controlling the actions or operations of a computer, operating, network and/or communications system.

5.1.4. **Virus and Malicious Code** - A set of instructions or programming code which reproduces its own code by attaching itself to other programs in such a way that the virus code is executed when the infected program is executed. This is usually performed without the permission or knowledge of the user causing damage to information and data. Viruses can be transmitted by downloading code from an external source such as web-sites, code attached to an e-mail, or it may be present on a diskette or CD that is brought in from the outside. The virus may lie dormant until circumstances cause its code to be executed by the computer. See P800-S860, GITA's state-wide Virus and Malicious Code Protection Standard for a description of virus types.

5.2 **Abbreviations and Acronyms**

5.2.1 **DES** – **D**epartment of **E**conomic **S**ecurity
5.2.2 **DSS** – **D**atacenter **S**erver **S**upport
5.2.3 **DTS** – **D**ivision of **T**echnology **S**ervices
5.2.4 **GITA** – **G**overnment **I**nformation **T**echnology **A**gency
5.2.5 **IT** – **I**nformation **T**echnology
5.2.6 **CIO** – **C**hief **I**nformation **O**fficer

6. STANDARD

6.1. Network Associates/McAfee will be used on all servers and on all workstations.

6.2. All anti-virus engines and dats shall be updated at least weekly. Local LAN Administrators are responsible for standalone PC workstations.

6.3. If weekly updates are no longer available from the software manufacturer (Network Associates/McAfee), this standard must be reviewed within 90 days to identify other standard anti-virus software products.

6.4. All DES divisions and programs shall implement anti-virus programs that are compliant with this standard on their computers, operating, network, and communication systems.

6.5. Information entering the DES network from the Internet must be checked for viruses. This function will be administered by DTS DSS, and will occur at the firewall at the web server level.

6.6. If viruses affect DES' e-mail systems, networks, operating systems, communication systems, information, data and/or programs, DES staff shall remedy the problem as quickly as possible through anti-virus programs and all other resources available, internal or external, to the agency. Please refer to 1-38-0052, the *DES Virus Procedures*.

6.7. DES provides capabilities for remote users to access DES systems. Each user must understand and agree that access rights are a privilege which can be revoked if diligence is not exercised in protecting their remote devices from viruses. Remote access users will comply with minimum DES standards as follows:

6.7.1. All DES equipment used for remote access will comply with current DES virus protection standards. McAfee anti-virus software is required on all remote machines.

6.7.2. All remote anti-virus engines and dats shall be updated at least weekly.

STANDARD (continued)

6.7.3. All non-DES equipment used for remote access to DES resources (including, but not limited to: personally owned PCs and PCs owned by vendors, service providers, other government entities, and anyone else that has been granted access to DES IT resources) will either conform to the DES standard for virus protection or provide a functional equivalent that has the same or better protection. Decisions about alternative protection systems' equivalency to DES standards will be made by DES.

6.7.4. Disabling virus protection systems and/or disregarding DES virus protection policies and standards may result in remote access privileges being revoked.

6.8 Update Rules – Only software patches sanctioned by the manufacturer (vendor) of the software being patched may be applied.

7. **Implications**

7.1. DES is responsible for the protection of its information assets. It is DES' responsibility to purchase, maintain, and upgrade necessary anti-virus programs for the prevention of infection and/or infected systems.

7.2. Some DES divisions may need to invest in appropriate software, staff, and/or infrastructure to keep the software current and within this standard.

8. **Implementation Strategy**

8.1. All DES divisions and programs will implement this standard.

8.2. An exception may be granted by the DES CIO to use a different virus protection product if the current DES standard product is not compatible with other products used to provide ADA related services.

8.3. An exception may be granted by the DES CIO to use a different virus protection product if a DES business unit purchases equipment or software for a non-DES entity and that entity has a different virus protection standard and provides its own support services.

9. **References**

9.1. 1-38-0013 DES Virus and Malicious Code Policy
9.2. 1-38-0015 DES Internet Use Policy
9.3. 1-38-0052 DES Virus Procedures

10. **Attachments**

10.1. None

11. **Associated GITA IT Standards or Policies**

11.1. P800-S860 Virus and Malicious Code Protection Standard

12. **Review Date**

12.1. This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.